

ATTORNEY DOCKET
016295.0858
(DC-01605)

PATENT APPLICATION
09/237,016

FAX RECEIVED

JUN 24 2003

1

PETITIONS OFFICE

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

La Vaughn F. Watts Jr. et al.

Serial No.:

09/237,016

Date Filed:

January 25, 1999

Examiner:

Jackson, Jenise E.

Group Art Unit:

2131

Title:

*Portable Computer System with Hierarchial
and Token-Based Security Policies*

BOX DAC
OFFICE OF PETITIONS
Honorable Assistant Commissioner
of Patents
Washington, D.C. 20231

I hereby certify that this
correspondence is being transmitted
via facsimile transmission to
703.308.6916, BOX DAC, Assistant
Commissioner of Patents, P.O. Box
1450, Alexandria, VA 22313-1450 on
the date shown below.

K. M. Blease

Kamishia Blease

6/24/03

Date

Dear Sir:

RECEIVED

JUN 27 2003

NON-FEE PETITION UNDER 37 C.F.R. § 1.181
TO WITHDRAW HOLDING OF ABANDONMENT

Technology Center 2100

OR

IN THE ALTERNATIVE, PETITION TO REVIVE UNINTENTIONALLY
ABANDONED APPLICATION UNDER 37 C.F.R. 1.137(B)

Applicant believes that his request in filing the Non-Fee Petition Under 37 C.F.R. § 1.181 To Withdraw Holding Of Abandonment is applicable to this particular case. However, in the alternative, Applicant is also filing the Petition to Revive Unintentionally Abandoned Application under 37 C.F.R. 1.137(B) to eliminate any delays.

RECEIVEDATTORNEY DOCKET
016295.0858
(DC-01605)

JUN 27 2003

Technology Center 2100

PATENT APPLICATION
09/237,016

FAX RECEIVED

JUN 24 2003

2

PETITIONS OFFICE

**Non-Fee Petition Under 37 C.F.R. § 1.181
to Withdraw Holding of Abandonment**

This non-fee petition is filed in response to a June 2, 2003, telephone call from the Examiner. The Examiner indicated that a response to the present application has lapsed and the application is considered abandoned due to Applicants' failure to timely file a proper response to the Final Office Action letter mailed on October 23, 2002. However, Applicants had filed a timely and proper response to the Final Office Action on December 23, 2002. Applicants believe that the Response to the Final Office Action is fully responsive to the Final Office Action and as such places the application in a condition for allowance.

Enclosed is a copy of the "Response to Final Office Action" filed December 23, 2002, by Express Mail Post Office to Addressee service under the provisions of 37 C.F.R. 1.10. Also attached is a copy of the Delivery Status of Applicants' Express Mail to the U.S. Patent and Trademark Office evidencing receipt of the Response on December 26, 2002. Further attached is a copy of Applicants' postcard returned by the U.S. Patent and Trademark Office evidencing receipt of the Response indicating the filing date of December 23, 2002.

Although Applicants have yet to receive the notification by the U.S. Patent and Trademark Office that the above-referenced patent application has been abandoned for failure to file a timely and proper reply to the Final Office Action mailed October 23, 2002, Applicants have received the Advisory Action mailed June 15, 2003, and believe the abandonment notice will be issued in due course. This Petition under 37 C.F.R. § 1.181 is to request that the holding of abandonment be withdrawn.

**In the Alternative, Petition to Revive Unintentionally
Abandoned Application Under 37 C.F.R. 1.137(B)**

Although Applicants believe that his request in filing the non-fee petition as referenced above is applicable to this particular case, Applicants are also filing the Petition to Revive Unintentionally Abandoned Application Under 37 C.F.R. 1.137(B) to eliminate any delays.

The six-month deadline for filing a Response to the Final Office Action dated October 23, 2002, was April 23, 2003. Applicants have yet to receive an official notice of abandonment from the U.S. Patent and Trademark Office. Although Applicants filed a

ATTORNEY DOCKET
016295.0858
(DC-01605)

PATENT APPLICATION
09/237,016

3

response to the Final Office Action within two months of the mailing date of the Final Office Action, Applicants believe the application became abandoned on April 23, 2003 as a matter of law. The entire delay in filing the required reply from the due date for the reply until the filing of this grantable petition under 37 C.F.R. 1.137(b) was unintentional.

If it is determined that a petition to revive unintentionally abandoned application under 37 C.F.R. 1.137(b) is required, this reply includes a Request for Continued Examination and Amendment with Transmittal and an authorization for the U.S. Patent and Trademark Office to deduct such filing fees from the listed deposit account for the RCE fee required under 37 C.F.R. § 1.17(e). Although Applicants filed a reply to the Final Office Action within two (2) months of the mailing date of the final action, the Examiner did not mail an Advisory Action until June 15, 2003.

Conclusion

Applicants believe there are no fees due, however, if it is determined that a petition fee or any additional fees or extensions are due, the Commissioner is hereby authorized to charge any additional fees or credit any overpayment for this paper to Deposit Account No. 02-0383 of BAKER BOTTS L.L.P.

Respectfully submitted,
BAKER BOTTS L.L.P.
Attorneys for Applicant



Patrick J. Porter
Reg. No. 45,658

Date: 24 June 2003

Customer No. 23640

512.322.2690
512.322.8385 (Fax)

RECEIVED

JUN 27 2003

Technology Center 2100

The "Received" stamp of the Patent and Trademark Office imprinted hereon acknowledges the filing of:

Application - Spec., Claims, Abstract (___ Page(s))		<input type="checkbox"/> Verified Statement (___ Page(s))
<input type="checkbox"/> CIP	<input type="checkbox"/> Conv. Prov.	<input type="checkbox"/> ___ Mo. Extension of Time (___ Page(s))
<input type="checkbox"/> Cont.	<input type="checkbox"/> Provisional	<input checked="" type="checkbox"/> Amendment/Response (19 Page(s))
<input type="checkbox"/> Informal/Formal Drawing(s) (___ Page(s))		<input type="checkbox"/> Issue Fee Transmittal (___ Page(s))
Declaration(s)/Power(s) of Attorney (___ Page(s))		<input type="checkbox"/> Check No. ___ Amt.: \$
<input type="checkbox"/> Executed <input type="checkbox"/> Unexecuted		<input checked="" type="checkbox"/> Check No. ___ Amt.: \$
<input type="checkbox"/> Assignment w/ or w/o Cover Sheet (___ Page(s))		<input type="checkbox"/> Other:
<input type="checkbox"/> IDS and PTO-1449 (___ Page(s))		
<input type="checkbox"/> w/Refs. <input type="checkbox"/> w/o Refs.		
<input type="checkbox"/> Non-Publication Request (___ Page(s))		

Inventor(s): La Vaugh F. Watts Jr. et al.	Serial No.: 09/237,016
---	------------------------

Receipt Date & Serial No.:

Title: Portable Computer System with Hierarchical and Token-Based Security Policies

Client/Applicant: Dell Computer	BB File No.: 016295.0858
---------------------------------	--------------------------

Mailed: 12/23/02

Certificate of Mailing

Due:

☒ Express Mail Rept No.: EV141763226US

Atty./Secy.: TRF/kwc

☐ First Class Mail☐ Hand Delivered

[Home](#)

Track & Confirm

Delivery Status

You entered EV14 1763 226U S

Your item was delivered at 7:50 am on December 26, 2002 in WASHINGTON, DC 20231 to PATENT OFFICE 20231. The item was signed for by T T FORD.

[Shipment History >](#)[Request Delivery Record >](#)

Track & Confirm

Enter label number:

[Go >](#)[Track & Confirm FAQs](#)[Go >](#)

POSTAL INSPECTORS
Preserving the Trust

[site map](#) [contact us](#) [government services](#)
Copyright © 1999-2002 USPS. All Rights Reserved. [Terms of Use](#) [Privacy Policy](#)



FAX RECEIVED

001/026

BAKER BOTTS LLP

Fax receipt will not be confirmed by phone unless requested.

JUN 24 2003

PETITIONS OFFICE

FAX RECEIVED
JUN 23 2003
CANCELLED
PETITIONS OFFICE1500 SAN JACINTO CENTER
98 SAN JACINTO BOULEVARD
AUSTIN, TEXAS
78701-4039
512.322.2500
FAX 512.322.2501
www.bakerbotts.comAUSTIN
BAKU
DALLAS
HOUSTON
LONDON
MOSCOW
NEW YORK
RIYADH
WASHINGTON

TO Office of Petitions

FAX NO. 703.308.6916

FIRM/COMPANY U.S. Patent & Trademark Office

VOICE NO.

FROM Patrick J. Porter

VOICE NO. 512.322.2690

DATE June 24, 2003

RETURN TO Kamishia Blease

PERSONAL FAX NO. 512.322.8385

PAGES (including cover) 26

MESSAGE

Re: 09/237,016

RECEIVED

JUN 27 2003

Technology Center 2100

Notice of Confidentiality

The information contained in and transmitted with this facsimile is: 1. Subject to the Attorney-client Privilege; 2. Attorney Work Product; or 3. Confidential. It is intended only for the individual or entity designated above. You are hereby notified that any dissemination, distribution, copying, or use of or reliance upon the information contained in and transmitted with this facsimile by or to anyone other than the recipient designated above by the sender is unauthorized and strictly prohibited. If you have received this facsimile in error, please notify Baker Botts L.L.P. by telephone at 512.322.2575 immediately. Any facsimile erroneously transmitted to you should be immediately returned to the sender by U.S. Mail or, if authorization is granted by the sender, destroyed.

If you do not receive all pages, please call: 512.322.2575 for assistance.

ATTORNEY DOCKET
016295.0858
(DC-01605)

FAX RECEIVED
JUN 24 2003
PETITIONS OFFICE

PATENT APPLICATION

09/237,016

~~CANCELLED~~
FAX RECEIVED
JUN 23 2003
PETITIONS OFFICE

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

Serial No.:

Date Filed:

Examiner:

Group Art Unit:

Title:

La Vaughn F. Watts Jr. et al.

09/237,016

January 25, 1999

Jackson, Jenise E.

2131

RECEIVED

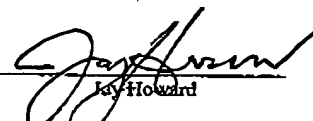
JUN 27 2003

Technology Center 2100

*Portable Computer System with Hierarchical
and Token-Based Security Policies*

BOX AF
Honorable Assistant Commissioner
of Patents
Washington, D.C. 20231

I hereby certify that this
communication is being deposited
with the United States Postal
Service as Express Mail No.
EV141763226US addressed to:
Box AF, Assistant Commissioner
of Patents, Washington, D.C.
20231, on the date shown below.


Jay Howard
12-23-02
Date

Dear Sir:

EV141763226US

RESPONSE TO FINAL OFFICE ACTION

In response to the Final Office Action, mailed October 23, 2002, Applicants request that the Examiner reconsider the rejections of the claims in view of the following amendments and remarks.

ATTORNEY DOCKET
016295.0858
(DC-01605)

PATENT APPLICATION
09/237,016

2

AMENDMENTS

For the convenience of the Examiner, all pending claims of the present application are shown below in clean form whether or not an amendment has been made. Please refer to the attached sheet showing a mark-up version of the amendments to the claims.

IN THE CLAIMS:

1. (Twice Amended) A computer system comprising:
 - a processor;
 - an access token communicator capable of being coupled to the processor, the access token communicator being adapted to read an access token;
 - an input device capable of being coupled to the processor, the input device being adapted to receive a security code, the security code confirming authorized use of the access token;
 - a software system executable on the processor and including a system security process controlling operational access to the processor, the software system including:
 - an executable program code that accesses the access token and the security code;
 - an executable program code that verifies validity of the access token by comparing the security code to a verification data on the access token, whereby if the security code matches verification data the access token is valid;
 - an executable program code that receives a set of security policies from the access token in the processor if the access token is valid; and
 - an executable program code that controls access to resources in the processor based on the security policies.
2. (Twice Amended) The computer system of claim 1 further comprising:
 - a nonvolatile storage device operably coupled to the processor;
 - a nonvolatile storage device access password that selectively allows access to the nonvolatile storage device, wherein the nonvolatile storage device password is supplied in response to the executable program code verifying that the security code matches the verification data on the access token.

ATTORNEY DOCKET
016295.0858
(DC-01605)

PATENT APPLICATION
09/237,016

3

3. (Previously Amended) The computer system of claim 2, wherein at least one of the set of security policies is stored within the nonvolatile storage device password.

4. (Previously Amended) The computer system of claim 1, wherein at least one of the set of security policies is stored on the access token.

5. (Previously Amended) The computer system of claim 1 wherein one of the set of security policies corresponds to the verification data.

6. (Previously Amended) A computer system comprising:
a processor;
an access token communicator capable of being coupled to the processor, the access token communicator being adapted to read an access token;
an input device capable of being coupled to the processor, the input device being adapted to receive verification data, the verification data confirming authorized use of the access token;
a software system executable on the processor and including a system security process controlling operational access to the processor, the software system including:
an executable program code that accesses the access token and the verification data;
an executable program code that verifies validity of the access token using the verification data;
an executable program code that sets security policies in the processor, wherein one of the one or more policies includes a BIOS control information that is used to configure the computer system; and
an executable program code that controls access to resources in the processor based on the security policies.

7. (Previously Amended) The computer system of claim 6 wherein the BIOS control information further includes password change information, the password change information including one or more password change settings for a user using the one or more security policies.

ATTORNEY DOCKET
016295.0858
(DC-01605)

PATENT APPLICATION
09/237,016

4

8. (Twice Amended) A computer system comprising:
- a processor;
 - an access token communicator capable of being coupled to the processor, the access token communicator being adapted to read an access token;
 - an input device capable of being coupled to the processor, the input device being adapted to receive verification data, the verification data confirming authorized use of the access token;
 - a software system executable on the processor and including a system security process controlling operational access to the processor, the software system including:
 - an executable program code that accesses the access token and the verification data;
 - an executable program code that verifies validity of the access token using the verification data;
 - an executable program code that sets security policies in the processor;
 - an executable program code that controls access to resources in the processor based on the security policies; and
 - a display device, wherein one of the one or more security policies includes one or more interface settings that control a desktop presentation on the display device.
9. The computer system of claim 2 wherein a password corresponding to the nonvolatile storage device access password is stored on the access token.
10. The computer system of claim 2 wherein one or more bytes of the nonvolatile storage device access password are in a non-keyboard enterable format.
11. The computer system of claim 1 wherein the access token includes one or more bytes of data in a non-keyboard enterable format.
12. The computer system of claim 1 wherein the verification data includes biometric data supplied by a user.

ATTORNEY DOCKET
016295.0858
(DC-01605)

PATENT APPLICATION
09/237,016

5

13. The computer system of claim 1 wherein the input device includes a keyboard and the verification data includes a personal identification number.

Please cancel Claim 14 without prejudice or disclaimer.

15. (Twice Amended) A computer system comprising:
one or more processors;
memory electrically interconnected to the one or more processors;
an operating system for controlling the operation of the one or more processors;
an access token communication device electrically interconnected to at least one of the one or more processors, the access token communication device being communicatively operable with an access token;
an input device electrically interconnected to at least one of the one or more processors, the input device operable to transmit a security code from a user to the one or more processors;
a nonvolatile storage device electrically interconnected to at least one of the one or more processors, the nonvolatile storage device including a nonvolatile memory;
a set of security policies associated with the operating system, the operating system operable to receive the security code for selectively enabling the set of security policies to limit access to the computer system; and
the operating system permitting access to the nonvolatile storage device and the one or more processors if the security code and the set of security policies match an authorization data stored in the nonvolatile memory,
wherein the access token further includes verification data, the verification data operable to provide the security policies to the nonvolatile memory if the security code matches an authentication code stored in the access token.

16. (Twice Amended) The computer system of claim 15 wherein the operating system includes a BIOS and the BIOS is stored in the nonvolatile memory that is electrically interconnected to the one or more processors.

ATTORNEY DOCKET
016295.0858
(DC-01605)

PATENT APPLICATION
09/237,016

6

17. (Amended) The computer system of claim 15 wherein the access token communication device includes a smart card communication device.

18. (Amended) The computer system of claim 15 wherein the access token communication device includes network circuitry that is adapted to receive signals from one or more computers interconnected on a computer network.

19. (Amended) The computer system of claim 15 wherein the access token communication device includes a modem that receives signals from a communications line.

20. (Amended) The computer system of claim 15 wherein the input device is a keyboard.

21. (Amended) The computer system of claim 15 wherein the input device includes a biometric data reading device.

22. (Amended) The computer system of claim 15 wherein the biometric data reading device includes a fingerprint scanner.

23. (Amended) The computer system of claim 15 wherein the biometric data reading device includes a retinal scanning device.

24. (Amended) The computer system of claim 15 wherein the nonvolatile storage device includes a hard disk drive.

25. (Amended) The computer system of claim 15 further comprising a data access code stored in the nonvolatile memory, wherein a data request code corresponding to the data access code alters a state of the nonvolatile storage device.

26. (Previously Amended) A method for accessing a computer system, said method comprising:

ATTORNEY DOCKET
016295.0858
(DC-01605)

PATENT APPLICATION
09/237,016

7

providing a computer system, the computer system including:

- one or more processors;
- a memory operably coupled to the one or more processors;
- an operating system for controlling the operation of the one or more processors;
- an access token reading device that is adapted to read information stored on an access token;
- an input device that is adapted to transmit verification data to the operating system, the verification data confirming authorized use of the access token;
- a nonvolatile storage device operably coupled to the memory;
- a nonvolatile storage device access password that selectively allows access to the nonvolatile storage device, wherein the nonvolatile storage device password is supplied in response to the access token reading device reading an access token and the input device receiving verification data;
- storing a master password on the access token;
- storing a nonvolatile storage device password on the access token; and
- comparing the verification data to the master password and the nonvolatile storage device password for access to the computer system.

27. The method of claim 26 further comprising:

- storing a password corresponding to the nonvolatile storage device password on the nonvolatile storage device.

28. (Previously Amended) A method for protecting information stored in an information handling system, said method comprising:

- reading an access token containing a security policy for the information handling system;
- requesting an authentication password from a user;
- authenticating the use of the access token by comparing the password to the security policy;
- setting a security policy in the information handling system; and
- unlocking a nonvolatile storage device on the information handling system.

ATTORNEY DOCKET
016295.0858
(DC-01605)

PATENT APPLICATION
09/237,016

8

29. (Previously Amended) A method for assembling a computer system, said method comprising:

receiving a list of components for assembling the computer system;
receiving one or more security policies;
configuring the computer system using the one or more security policies; and
accessing the computer system with a user input password combined with a token access password such that the combined passwords match the one or more security policies configured in the computer system.

30. The method of claim 29 further comprising:
initializing a system password installed on the computer system.

31. The method of claim 29 further comprising:
providing a nonvolatile storage device for the computer system, wherein the nonvolatile storage device includes a nonvolatile storage device password; and
initializing the nonvolatile storage device password.

32. The method of claim 29 wherein the configuring includes modifying a nonvolatile memory installed in the computer system.

33. The method of claim 29 further comprising:
retaining a copy of the nonvolatile storage device password at a location removed from the computer system.

34. (Previously Amended) The method of claim 29 further comprising:
configuring an access token for the computer system, the access token including the security policies and the passwords associated with the computer system.

35. (Twice Amended) A method of using an access token, said method comprising:

ATTORNEY DOCKET
016295.0858
(DC-01605)

PATENT APPLICATION
09/237,016

9

transferring one or more passwords from the access token to a computer system;
receiving a user input password at the computer system; and
matching a computer system password with the user input password with the one or more passwords from the access token to access the computer system, wherein the computer system password includes one or more security policies configured in the computer system.

36. (Previously Amended) The method of claim 35 wherein the transferring step is performed in response to an access code received by the access token.

37. The method of claim 35 wherein one of the one or more passwords corresponds to a computer system password installed on the computer system.

38. The method of claim 35 wherein one of the one or more passwords corresponds to a nonvolatile storage device password installed on a nonvolatile storage device.

Claim 39 previously cancelled without prejudice or disclaimer.

40. (Amended) A communication device having an access token for use with a computer system, said communication device comprising:

one or more security policies adapted to be used by the computer system, wherein the one or more security policies are stored in an encrypted format; and

a security code stored on the access token, wherein the communication device transmits the one or more security policies in response to receiving an authentication code corresponding to the security code.

41. (Twice Amended) A computer operable medium for protecting a computer system, said computer operable medium comprising:

means for reading an access token containing a security policy for the computer system;

means for receiving an authentication password from a user;

ATTORNEY DOCKET
016295.0858
(DC-01605)

PATENT APPLICATION
09/237,016

10

means for verifying the validity of the access token based on a comparison of the authentication password to the security policy;

means for setting security policies in the computer system; and

means for unlocking a nonvolatile storage device on the computer system.

42. (Twice Amended) An information handling system comprising:

means for reading an access token containing a security policy for the information handling system;

means for receiving an authentication password from a user;

means for verifying the validity of the access token based on a comparison of the authentication password to the security policy;

means for setting security policies in the information handling system; and

means for unlocking a nonvolatile storage device on the information handling system.

REMARKS

Applicants have carefully reviewed this application in light of the Final Office Action mailed October 23, 2002. Claims 1-38 and 40-42 are pending in this application. Claims 1-5, 9-14, 16-25, and 35-38, 40-42 are rejected. Claims 6-8 and 26-34 are allowed and Claim 15 is objected to as being dependent upon a rejected claim. Applicants previously cancelled Claim 39 without prejudice or disclaimer. Applicants have amended Claims 1, 2, 8, 15-25, 35, and 40-42 to further define that which Applicants regard as their invention and respectfully request reconsideration and favorable action in this case.

Rejections under 35 U.S.C. § 101

Claim 40 stands rejected by the Examiner under 35 U.S.C. § 101 as not constituting statutory subject matter. Applicants respectfully traverse and submit that amended Claim 40 is patentable. Applicants respectfully request reconsideration and withdrawal of the rejection and allowance of amended Claim 40.

Objected Claims

Claim 15 is objected to by the Examiner as being dependent on a rejected base claim. Applicants have amended Claim 15 to include the limitations of the base claim. Applicants request withdrawal of the objection and allowance of amended Claim 15.

ATTORNEY DOCKET
016295.0858
(DC-01605)

PATENT APPLICATION
09/237,016

11

Rejections under 35 U.S.C. § 103

Claims 1-5, 9-14, 16-25, 35-38, 40-42 stand rejected by the Examiner under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 5,949,882 issued to Michael F. Angelo (hereinafter "Angelo") and Authoritative Dictionary of IEEE Standards (hereinafter "IEEE Standards") in view of U.S. Patent No. 6,282,649 issued to Howard Shelton Lambert (hereinafter "Lambert"). Applicants have Claim 14 without prejudice or disclaimer. Applicants respectfully traverse and submit that Claims 1-5, 9-13, 16-25, 35-38, and 40-42, as amended, are patentable over Angelo and IEEE Standards in view of Lambert.

Angelo discloses a two piece authentication procedure to enable access to secured computer resources (col. 3, lines 30-31). The procedure uses a token or smart card "to store an encryption algorithm furnished with an encryption key that is unique or of limited production" (col. 3 lines 37-39). The encryption algorithm is used to encrypt a user-entered password to create a "peripheral" password to permit access to the secured resource (col. 3, lines 41-48).

Lambert discloses an access control system that utilizes hierarchical user keys, which have different access keys for different access levels.

Applicants' amended Claim 1 calls for various features including "an executable program code that verifies validity of the access token by comparing the security code to a verification data on the access token, whereby if the security code matches verification data the access token is valid."

Applicants' amended Claim 35 recites, in part, "matching a computer system password with the user input password with the one or more passwords from the access token to access the computer system, wherein the computer system password includes one or more security policies configured in the computer system."

Applicants' amended Claim 40 calls for various features including "a security code stored on the access token, wherein the communication device transmits the one or more security policies in response to receiving an authentication code corresponding to the security code."

Applicants' amended Claim 41 calls for various features including "means for reading an access token containing a security policy for the computer system," and "means for

ATTORNEY DOCKET
016295.0858
(DC-01605)

PATENT APPLICATION
09/237,016

12

verifying the validity of the access token based on a comparison of the authentication password to the security policy.”

Applicants’ amended Claim 42 calls for various features including “means for reading an access token containing a security policy for the information handling system,” and “means for verifying the validity of the access token based on a comparison of the authentication password to the security policy.”

Neither Angelo, IEEE Standards, nor Lambert make obvious Claims 1-5, 9-13, 35-38 and 40-42, as amended, of Applicants’ invention because Angelo, IEEE Standards, or Lambert fails to teach disclose, or suggest all of the elements recited in Claims 1-5, 9-13, 35-38 and 40-42, as amended. For example, the cited references fail to disclose “an executable program code that verifies validity of the access token by comparing the security code to a verification data on the access token, whereby if the security code matches verification data the access token is valid” as recited in amended Claim 1. As further recited in amended Claim 35, Angelo, IEEE Standards, or Lambert fails to disclose, suggest, or teach “matching a computer system password with the user input password with the one or more passwords from the access token to access the computer system, wherein the computer system password includes one or more security policies configured in the computer system.”

As further recited in amended Claim 40, Angelo, IEEE Standards, or Lambert fails to disclose, suggest, or teach “a security code stored on the access token, wherein the communication device transmits the one or more security policies in response to receiving an authentication code corresponding to the security code.” As recited in amended Claim 41, Angelo, IEEE Standards, or Lambert fails to disclose, suggest, or teach “means for reading an access token containing a security policy for the computer system,” and “means for verifying the validity of the access token based on a comparison of the authentication password to the security policy.” As recited in amended Claim 42, Angelo, IEEE Standards, or Lambert fails to disclose, suggest, or teach “means for reading an access token containing a security policy for the information handling system,” and “means for verifying the validity of the access token based on a comparison of the authentication password to the security policy.” Applicants therefore respectfully request the Examiner to reconsider and withdraw the rejection to and allow amended Claims 1, 35 and 40-42.

ATTORNEY DOCKET
016295.0858
(DC-01605)

PATENT APPLICATION
09/237,016

13

Claims 2-5 and 9-13, as amended, directly or indirectly depend from and provide further patentable limitations to amended Claim 1. Amended Claims 16-25 directly or indirectly depend from and provide further patentable limitations to Claim 15. Claims 36-38 directly or indirectly depend from and provide further patentable limitations to Claim 35. Because Claims 6, 15, and 35, as amended, are deemed allowable, Claims 2-5, 9-13, 16-25, and 36-38, as amended, are allowable. Therefore, Applicants respectfully request the Examiner to reconsider and withdraw the rejection to and allow Claims 1-5, 9-13, 16-25, 35-38, and 40-42, as amended.

Allowable Subject Matter

Applicants appreciate the Examiner's careful review of the application and allowance of Claims 6-8 and 26-34.

CONCLUSION

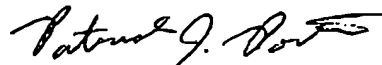
Applicants have now made an earnest effort to place this case in condition for allowance in light of the amendments and remarks set forth above. Applicants respectfully request reconsideration of the rejections and allowance of the claims, as amended.

Attached hereto is a marked-up version of the changes made to the specification and claims by the current amendments. The attached pages are captioned "Version with Markings to Show Changes Made."

Applicants believe no fee is due, however, the Commissioner is hereby authorized to charge any fees or credit any overpayments to Deposit Account No. 02-0383 of Baker Botts L.L.P.

Respectfully submitted,

BAKER BOTTS L.L.P.
Attorneys for Applicants



Patrick J. Porter
Reg. No. 45,658

Date: December 23, 2002
Correspondence Address:
One Shell Plaza
910 Louisiana
Houston, Texas 77002-4992
512.322.2690
512.322.8385 (Fax)

ATTORNEY DOCKET
016295.0858
(DC-01605)

PATENT APPLICATION
09/237,016

Version with Markings to Show Changes Made

1

IN THE CLAIMS:

Please cancel Claim 14, and amend Claims 1, 2, 8, 15-25, 35 and 40-42 as follows:

1. (Twice Amended) A computer system comprising:

a processor;

an access token communicator capable of being coupled to the processor, the access token communicator being adapted to read an access token;

an input device capable of being coupled to the processor, the input device being adapted to receive a security code [verification data], the security code [verification data] confirming authorized use of the access token;

a software system executable on the processor and including a system security process controlling operational access to the processor, the software system including:

an executable program code that accesses the access token and the security code [verification data];

an executable program code that verifies validity of the access token by comparing the security code to a verification data on the access token, whereby if the security code matches verification data the access token is valid [using the verification data];

an executable program code that receives a set of security policies from the access token in the processor if the access token is valid [in response to the verification data];
and

an executable program code that controls access to resources in the processor based on the security policies.

2. (Twice Amended) The computer system of claim 1 further comprising:

a nonvolatile storage device operably coupled to the processor;

a nonvolatile storage device access password that selectively allows access to the nonvolatile storage device, wherein the nonvolatile storage device password is supplied in response to the executable program code verifying that the security code matches the verification data on the access token. [receiving valid verification data with the access token provided.]

ATTORNEY DOCKET
016295.0858
(DC-01605)

PATENT APPLICATION
09/237,016

Version with Markings to Show Changes Made

2

verification data on the access token. [receiving valid verification data with the access token provided.]

8. (Twice Amended) A computer system comprising:

a processor;

an access token communicator capable of being coupled to the processor, the access token communicator being adapted to read an access token;

an input device capable of being coupled to the processor, the input device being adapted to receive verification data, the verification data confirming authorized use of the access token;

a software system executable on the processor and including a system security process controlling operational access to the processor, the software system including:

an executable program code that accesses the access token and the verification data;

an executable program code that verifies validity of the access token using the verification data;

an executable program code that sets security policies in the processor; [and]

an executable program code that controls access to resources in the processor based on the security policies; and

a display device, wherein one of the one or more security policies includes one or more interface settings that control a desktop presentation on the display device.

Please cancel Claim 14 without prejudice or disclaimer.

15. (Twice Amended) [The computer system of claim 14] A computer system comprising:

one or more processors;

memory electrically interconnected to the one or more processors;

an operating system for controlling the operation of the one or more processors;

ATTORNEY DOCKET
016295.0858
(DC-01605)

PATENT APPLICATION
09/237,016

Version with Markings to Show Changes Made

3

an access token communication device electrically interconnected to at least one of the one or more processors, the access token communication device being communicatively operable with an access token;

an input device electrically interconnected to at least one of the one or more processors, the input device operable to transmit a security code from a user to the one or more processors;

a nonvolatile storage device electrically interconnected to at least one of the one or more processors, the nonvolatile storage device including a nonvolatile memory;

a set of security policies associated with the operating system, the operating system operable to receive the security code for selectively enabling the set of security policies to limit access to the computer system; and

the operating system permitting access to the nonvolatile storage device and the one or more processors if the security code and the set of security policies match an authorization data stored in the nonvolatile memory,

wherein the access token further includes verification data, the verification data operable to provide the security policies to the nonvolatile memory if the security code matches an authentication code stored in the access token.

16. (Twice Amended) The computer system of claim 15 [14] wherein the operating system includes a BIOS and the BIOS is stored in the nonvolatile memory that is electrically interconnected to the one or more processors.

17. (Amended) The computer system of claim 15 [14] wherein the access token communication device includes a smart card communication device.

18. (Amended) The computer system of claim 15 [14] wherein the access token communication device includes network circuitry that is adapted to receive signals from one or more computers interconnected on a computer network.

ATTORNEY DOCKET
016295.0858
(DC-01605)

PATENT APPLICATION
09/237,016

Version with Markings to Show Changes Made

4

19. (Amended) The computer system of claim 15 [14] wherein the access token communication device includes a modem that receives signals from a communications line.

20. (Amended) The computer system of claim 15 [14] wherein the input device is a keyboard.

21. (Amended) The computer system of claim 15 [14] wherein the input device includes a biometric data reading device.

22. (Amended) The computer system of claim 21 [14] wherein the biometric data reading device includes a fingerprint scanner.

23. (Amended) The computer system of claim 21 [14] wherein the biometric data reading device includes a retinal scanning device.

24. (Amended) The computer system of claim 15 [14] wherein the nonvolatile storage device includes a hard disk drive.

25. (Amended) The computer system of claim 15 [14] further comprising a data access code stored in the nonvolatile memory, wherein a data request code corresponding to the data access code alters a state of the nonvolatile storage device.

35. (Twice Amended) A method of using an access token, said method comprising:

transferring one or more passwords from the access token to a computer system;
[and]

receiving a user input password at the computer system; and

matching a computer system password with [the combined user] the user input
password with the one or more passwords from the access token to access the computer

ATTORNEY DOCKET
016295.0858
(DC-01605)

PATENT APPLICATION
09/237,016

Version with Markings to Show Changes Made

5

system, wherein the computer system password includes one or more security policies configured in the computer system.

40. (Amended) [An] A communication device having an access token for use with a computer system, said [access token] communication device comprising:

one or more security policies adapted to be used by [a] the computer system, wherein the one or more security policies are stored in an encrypted format; and

[an access] a security code stored on the access token, wherein the communication device [access token] transmits the one or more security policies in response to receiving an authentication code [a data stream] corresponding to the [access] security code.

41. (Twice Amended) A computer operable medium for protecting a computer system, said computer operable medium comprising:

means for reading an access token containing a security policy for the computer system;

means for receiving an authentication password from a user;

means for verifying the validity of the access token based on a comparison of the authentication password to the security policy;

means for setting security policies in the [information handling] computer system; and

means for unlocking a nonvolatile storage device on the [information handling] computer system.

42. (Twice Amended) An information handling system comprising:

means for reading an access token containing a security policy for the information handling system;

means for receiving an authentication password from a user;

means for verifying the validity of the access token based on a comparison of the authentication password to the security policy;

ATTORNEY DOCKET
016295.0858
(DC-01605)

PATENT APPLICATION
09/237,016

Version with Markings to Show Changes Made

6

means for setting security policies in the information handling system; and
means for unlocking a nonvolatile storage device on the information handling system.